Вісник Львівського університету. Серія філос.-політолог. студії. 2024. Випуск 57, с. 88–97
Visnyk of the Lviv University. Series Philos.-Political Studies. Issue 57, p. 88–97

УДК 355.45:004.9](477)
DOI https://doi.org/10.30970/PPS.2024.57.12

ГІБРИДНІ ЗАГРОЗИ ЯК НОВИЙ ВИКЛИК НАЦІОНАЛЬНІЙ БЕЗПЕЦІ В ЕПОХУ ІНФОРМАЦІЙНИХ ВОЄН

Андрій Крап
ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом», кафедра суспільно-гуманітарних та фундаментальних дисциплін
вул. Фрометівська, 2, 03039, м. Київ, Україна

Стаття присвячена аналізу феномена гібридних загроз як свого роду комплексного (складеного) виклику національній безпеці в умовах сучасної епохи інформаційних війн. Метою дослідження, відповідно, є концептуальне (категоріальне) осмислення гібридних загроз, визначення їхньої природи, основних форм прояву, наслідків та розробка стратегій ефективної протидії. Особливу увагу приділено специфіці впливу гібридних загроз на державні інституції (а також на економічну стабільність та інформаційну сферу).

У процесі дослідження використано міждисциплінарний підхід, що інтегрує методи системного аналізу, історико-генетичного методу, порівняльного аналізу та критичного осмислення нормативно-правових засад. Завдяки саме такій конфігурації методологічного інструментарію, як видається, вдалося сформувати цілісне уявлення про багатовекторний характер гібридних загроз і окреслити шляхи їхньої нейтралізації.

Основними результатами статті є характеристика багатовимірної природи гібридних загроз; аналіз основних форм їх прояву (військової, інформаційної, економічної та кіберскладової); визначення наслідків гібридних загроз для національної безпеки; огляд міжнародного досвіду протидії (на прикладі ЄС, НАТО та Естонії) та його адаптація до українського контексту, а також пропозиції щодо інтеграції цифрових технологій у національні стратегії безпеки.

Наукова новизна статті полягає у формуванні комплексного підходу до вивчення гібридних загроз та розробці рекомендацій щодо їх ефективної нейтралізації. Теоретичне значення роботи полягає в узагальненні та систематизації сучасних концепцій гібридних загроз, що сприяє подальшому розвитку цієї тематики в наукових дослідженнях. Практичне значення полягає у формуванні рекомендацій для вдосконалення державної політики у сфері національної безпеки.

Ключові слова: гібридні загрози, національна безпека, інформаційна війна, кібербезпека, дезінформація, міжнародна співпраця, цифрові технології.

Постановка проблеми. Гібридні загрози, які постали перед сучасними державами, зокрема в контексті розгортання інформаційних воєн, унаочнюють нову фазу еволюції національної безпеки, що характеризується синергетичним поєднанням військових, економічних, інформаційних та кібертехнологій. На наше міркування, аналіз цього феномену вимагає глибокого осмислення не лише його структурної складової, а й функціонального впливу на політичну стабільність та суспільну свідомість, що, вочевидь, є ключовим у формуванні державної стратегії протидії.

У сучасному світі, що дедалі більше взаємозалежний, гібридні загрози постають не стільки як ізольовані виклики, скільки як комплексні системи, здатні підривати основи національного суверенітету через недекларовані форми агресії. Як видається, інформаційні війни, котрі використовуються в цьому контексті, слід розглядати не лише як інструмент дезінформації, але і як засіб маніпуляції масовою свідомістю, що перетворює інформацію

на зброю масового впливу (в умовах постійного збільшення обсягів інформаційних потоків це набуває особливого значення).

На наше переконання, визначення гібридних загроз як нового типу викликів національній безпеці потребує інтеграції міждисциплінарних підходів. Зокрема, підходи теорії систем (що дозволяють оцінювати взаємодію різних елементів у межах єдиної загрози), соціолінгвістичний аналіз (який сприяє розкриттю механізмів мовного впливу) та концепції міжнародних відносин (з акцентом на теорії балансу сил) мають становити основу такого дослідження. Гадаємо, що саме міждисциплінарний підхід дозволяє охопити всю складність проблеми, водночас сприяючи виробленню комплексних рішень.

З урахуванням викладеного вище, актуальність означеної тематики зумовлена не лише посиленням геополітичної нестабільності, але й необхідністю розроблення дієвих механізмів протидії, що враховують як національний контекст, так і глобальні виклики. Як видається, дослідження гібридних загроз потребує не лише аналізу їх проявів, але й критичного осмислення ролі держави, міжнародних організацій та суспільства у нейтралізації таких викликів, що й становить основну мету цієї роботи.

Аналіз останніх досліджень та публікацій. Дослідження гібридних загроз як феномена, що охоплює багаторівневий спектр викликів національній безпеці, активно розвивається, особливо у контексті інформаційних воєн, які стали характерною ознакою сучасної глобалізації. На наше міркування, багатогранність цієї тематики зумовлює необхідність систематичного аналізу наукових праць, які висвітлюють різні аспекти проблеми.

Окремі автори, як-от А. Шишацький та ін. [1, с. 26–29], наголошують на розробці методів ідентифікації гібридних викликів у системі управління національною безпекою. У їхніх дослідженнях підкреслено важливість інтеграції технологічних підходів, які дозволяють ефективно виявляти та нейтралізувати ці загрози. Як видається, їхній внесок є ключовим для розуміння базових принципів управління гібридними викликами.

М. Мітрович [2, с. 337–345] зосереджує увагу на концептуальних засадах гібридної безпеки, наголошуючи на сучасному підході до прогнозування загроз. З урахуванням викладеного вище, праці цього автора можна вважати теоретичним підґрунтям для аналізу специфіки гібридних викликів.

А. Братко, Д. Захарчук і В. Золька [3, с. 147–160] аналізують феномен гібридної війни, розглядаючи її як загрозу національній безпеці. У їхніх роботах підкреслено важливість міжнародного контексту, що, на наше міркування, є неодмінним елементом у розробці стратегій протидії. Ф. Дж. Сіллуффо та Дж. Р. Кларк [4, с. 46–63] пропонують аналіз гібридних загроз із позицій стратегічного мислення, розглядаючи їх як інтеграцію теоретичних і практичних підходів. Їхня робота допомагає зрозуміти природу цих загроз у контексті їхнього впливу на міжнародну політику. О. Царук і М. Корнієць [5, с. 57–78] акцентують на гібридній природі сучасних загроз у сфері кібербезпеки. Як видається, їхній внесок дозволяє поглибити розуміння того, як цифрові технології стають інструментом ведення гібридних воєн.

Н. Танеський і Р. Кіркова [6, с. 1795–1800] розробляють концептуальне бачення гібридних загроз, зосереджуючись на їхній складності та різноманітності форм прояву. Їхні міркування сприяють створенню більш цілісного уявлення про цей феномен. С. Білай та ін. [7, с. 1312–1321], а також К. Т. Іванівна та ін. [8, с. 163–175] розглядають питання управління і протидії гібридним загрозам у державному та громадському секторах. На наше переконання, їхній підхід до вдосконалення механізмів публічного управління заслуговує на окрему увагу. П. Каллен [9, с. 52–66] звертає увагу на приклади конкретних країн, таких як Австралія, що протистоять гібридним загрозам з боку Китаю. Ця робота є цінним джерелом для розуміння національних особливостей протидії таким викликам.

С. Санз-Кабальєро [10, с. 1–8] аналізує нормативно-правові засади регулювання гібридних загроз, приділяючи особливу увагу європейському контексту. Як видається, ця робота створює базу для формування правових стратегій протидії. Інші автори, як-от П. Балкан та ін. [11, с. 142–159], розглядають економічні аспекти гібридних загроз, зокрема через призму поділу тягаря їхньої протидії у межах міжнародних альянсів. На наше міркування, їхній підхід сприяє розумінню економічної складової цього явища.

Дослідження П., Лушенка С. Боса та С. Романюка [12, с. 83–93] пропонують концепцію інтеграції методів боротьби з повстанськими рухами для протидії гібридним загрозам. У своїй роботі автори підкреслюють, що стратегія боротьби з повстанцями може бути адаптована до гібридних викликів завдяки її орієнтації на локалізовані проблеми та здатності враховувати культурний і соціальний контексти. Як видається, ця модель є особливо корисною для розробки практичних рішень у контексті національної безпеки.

У дослідженні Н. А. М. Разалі та співавторів [13, с. 17151–17164] висвітлено використання гібридного підходу, що базується на лексичному аналізі та машинному навчанні, для прогнозування політичних загроз безпеці. На наше міркування, інноваційність цього підходу полягає в його здатності враховувати великі обсяги даних і створювати моделі прогнозування, які можуть застосовуватися для ідентифікації ранніх проявів гібридних загроз. С. Джаспер [14, с. 209–226] аналізує роль новітніх технологій у зміцненні стійкості проти гібридних загроз на прикладі російської агресії проти України. Автор наголошує на необхідності посилення співпраці між державними інституціями та приватними компаніями у сфері кібербезпеки. З урахуванням викладеного вище, це дослідження робить вагомий внесок у розуміння значення технологічного прогресу для протидії сучасним викликам.

К. Гарріс [15, с. 1784–1816] розглядає нестандартні гібридні загрози, зокрема діяльність таких організацій, як байкерські клуби, які використовуються як інструменти впливу. Це дослідження демонструє, наскільки гібридні загрози можуть виходити за межі традиційного розуміння та охоплювати нетипові суб'єкти. Дослідження С. Ч. Джунга та Е. В. Тана [16, с. 1–22] наголошує на ролі середніх держав, таких як Південна Корея, Сінгапур і Тайвань, у протидії гібридним загрозам через мінілатеральну співпрацю. На наше переконання, цей підхід дозволяє врахувати регіональні особливості та посилити колективну відповідь на загрози. Й. Шмід [17, с. 59–79] розглядає політичний ісламізм як одну з форм гібридної загрози, наголошуючи на складності та багатовимірності цього явища. Гадаємо, що його аналіз є важливим для вивчення взаємозв'язку ідеологічних і стратегічних аспектів у контексті сучасних викликів.

О. Сидорчук та співавтори [18, с. 747–759] досліджують вплив цифровізації на державне управління та його значення для забезпечення національної безпеки. Автори наголошують, що цифрові технології, хоча й створюють нові виклики, одночасно надають нові можливості для зміцнення безпеки та економічного розвитку.

Отже, дослідження, розглянуті в цьому огляді, висвітлюють широкий спектр аспектів гібридних загроз – від теоретичного аналізу до практичних стратегій протидії. На наше переконання, інтеграція цих підходів є необхідною для формування цілісного розуміння цього багатовимірного феномена. З урахуванням викладеного вище, дана стаття базується на синтезі кращих наукових ідей, що дозволяє запропонувати нові підходи до вивчення та нейтралізації гібридних викликів.

Метою статті є концептуальне осмислення феномена гібридних загроз як багатогранного виклику національній безпеці в умовах сучасної епохи інформаційних воєн, зокрема через аналіз їхньої природи, механізмів впливу та потенційних стратегій протидії. На наше переконання, дослідження спрямоване на виявлення структурних та

функціональних аспектів гібридних загроз, які інтегрують військові, інформаційні, економічні й технологічні компоненти, що впливають на стабільність державних інститутів та суспільства загалом.

Гадаємо, що важливим аспектом є також аналіз нормативно-правових, управлінських і соціально-політичних механізмів, які можуть забезпечити ефективну протидію таким викликам, враховуючи специфіку сучасних міжнародних відносин і технологічного прогресу. З урахуванням викладеного вище, мета роботи полягає у формуванні цілісного уявлення про природу гібридних загроз та розробці основних теоретичних і практичних підходів до їх нейтралізації в контексті забезпечення національної безпеки.

Виклад основного матеріалу. 1. Теоретико-методологічні засади дослідження гібридних загроз. Феномен гібридних загроз, що виник як результат еволюції сучасних конфліктів та використання новітніх технологій, характеризується багатовимірністю і складністю. Гібридні загрози є унікальним явищем, яке об'єднує традиційні військові, інформаційні, економічні та соціальні методи впливу, спрямовані на підрив національної безпеки та дестабілізацію суверенітету держави. На наше переконання, теоретичне осмислення цього явища вимагає інтеграції підходів різних наукових шкіл, зокрема системного аналізу, теорії міжнародних відносин і теорії інформаційних конфліктів [1, с. 26–29; 4, с. 46–63].

У широкому сенсі, гібридні загрози можуть бути визначені як комбінація традиційних і нетрадиційних методів впливу, що використовуються в єдиній стратегії. Як видається, ключовим аспектом гібридних загроз є їхня багатовекторність, що дозволяє атакувальній стороні адаптувати тактику залежно від специфіки цільової держави. На наше міркування, визначення багатовимірної природи таких загроз є важливим для розуміння їхніх механізмів впливу, адже вони охоплюють як видимі (військові дії, економічний тиск), так і приховані (інформаційні атаки, кібероперації) методи впливу [3, с. 147–160].

Системний аналіз, на нашу думку, є одним із базових методологічних підходів до вивчення гібридних загроз. Він дозволяє розглядати такі загрози як складні динамічні системи, де кожен компонент (військовий, інформаційний, економічний тощо) має свої специфічні функції, але водночас тісно взаємодіє з іншими елементами. У цьому контексті праця А. Шишацького та співавторів [1, с. 26–29] є показовою, адже автори запропонували модель ідентифікації гібридних викликів, яка враховує комплексний характер цих загроз.

Важливо також зазначити, що гібридні загрози активно використовують феномен асиметричних стратегій. Як наголошує М. Мітрович [2, с. 337–345], застосування таких стратегій дозволяє слабшим акторам конфлікту досягати значного впливу, уникаючи прямого зіткнення з сильнішими суперниками. Гадаємо, що цей підхід є особливо важливим у контексті сучасних міжнародних відносин, де нерівномірність розподілу сил і ресурсів стає ключовим фактором формування конфліктних сценаріїв.

Окрему увагу слід приділити інформаційному компоненту гібридних загроз, який стає дедалі важливішим у цифрову епоху. Інформаційні війни використовуються як засіб маніпулювання громадською свідомістю, підриву довіри до державних інституцій і створення хаосу у внутрішньому середовищі. Як зазначає О. Царук і М. Корнієць [5, с. 57–78], кіберзагрози та дезінформація є не лише інструментами, а й структурними елементами сучасних гібридних конфліктів. На наше переконання, аналіз цього компоненту є ключовим для розуміння трансформацій у сфері безпеки.

Інтеграція міждисциплінарних підходів, таких як історико-генетичний метод та аналіз міжнародних практик, дозволяє глибше розкрити еволюцію феномена гібридних загроз. Як видається, історичний контекст важливий для виявлення закономірностей зміни

форм та методів гібридних конфліктів. Наприклад, роботи С. Санз-Кабальєро [10, с. 1–8], які аналізують розвиток правового регулювання гібридних загроз у Європі, є цінними для розуміння правової основи цих викликів.

З урахуванням викладеного вище, теоретико-методологічні засади дослідження гібридних загроз ґрунтуються на системному, порівняльному та критичному аналізі, що дозволяє охопити багатогранність цього явища та сформувати цілісне бачення його природи. Гадаємо, що саме поєднання теоретичних знань і практичного досвіду є визначальним для розробки ефективних стратегій протидії.

2. Гібридні загрози в контексті національної безпеки: виклики та наслідки. У сучасному світі, що дедалі більше залежить від взаємодії держав, транснаціональних корпорацій і міжнародних організацій, гібридні загрози постають як одне з найсерйозніших випробувань для національної безпеки. Їхня природа полягає у поєднанні традиційних і новітніх засобів впливу, які, працюючи синхронно, здатні ефективно послаблювати державні інституції, маніпулювати суспільною думкою та дестабілізувати економічну систему. На наше переконання, багатовекторність цих загроз вимагає переосмислення підходів до забезпечення безпеки, зокрема в умовах сучасних інформаційних війн [1, с. 26–29].

2.1. Основні форми прояву гібридних загроз. Гібридні загрози мають багатоформатний характер, що проявляється у різноманітних сферах, від військової до інформаційної. Військова частина гібридних загроз залишається найпомітнішою, адже включає традиційні силові методи, такі як анексія територій, та асиметричні стратегії. Як зазначає М. Мітрович [2, с. 337–345], військові аспекти гібридних загроз є лише частиною загальної стратегії, яка водночас включає дезінформацію, економічний тиск та кібероперації.

Особливе місце серед форм прояву гібридних загроз займає інформаційна війна. Її основною метою є маніпулювання суспільною свідомістю, дискредитація уряду і створення паніки в суспільстві. Як вказують О. Царук і М. Корнієць [5, с. 57–78], дезінформація та інформаційні атаки сприяють підриву довіри до державних інституцій та суспільної злагоди, що робить їх ефективним інструментом у руках агресора. На наше міркування, ця форма загроз є однією з найскладніших для протидії через її невидимість і швидкість поширення.

Економічна частина гібридних загроз також заслуговує на окрему увагу. Вона охоплює такі методи, як введення санкцій, блокування торгових шляхів, маніпуляції на фінансових ринках або використання енергетичної залежності для впливу на політичні рішення держави. Роботи С. Санз-Кабальєро [10, с. 1–8] вказують на те, що економічні інструменти дедалі більше інтегруються у стратегії гібридних конфліктів, що підкреслює важливість їхнього правового регулювання.

Кіберзагрози, які є неодмінною частиною гібридних атак, становлять новий вимір сучасних конфліктів. Як зазначає С. Джаспер [14, с. 209–226], кібероперації дозволяють агресору проникати у критичну інфраструктуру, завдавати шкоди економічним та адміністративним системам, одночасно залишаючись непоміченими для традиційних механізмів оборони. На наше переконання, ця форма загроз стає дедалі більш небезпечною в умовах глобальної цифровізації.

2.2. Наслідки гібридних загроз для державної безпеки. Гібридні загрози мають деструктивний вплив на ключові аспекти функціонування держави. Військові аспекти таких загроз підривають територіальну цілісність та національний суверенітет. Як показує досвід України, агресор може використовувати різноманітні методи, починаючи від прямої військової інтервенції до інформаційних кампаній, спрямованих на деморалізацію населення [5, с. 57–78].

Одним із найсерйозніших наслідків є ерозія довіри до державних інституцій, яка виникає внаслідок дезінформації та поширення фейкових новин. Як зазначає К. Гарріс [15, с. 1784–1816], дискредитація уряду через інформаційні атаки створює хаос у внутрішньополітичному середовищі, послаблюючи спроможність держави до ефективного управління. На наше переконання, ці наслідки вимагають активного впровадження заходів, спрямованих на посилення інформаційної стійкості.

Економічний вплив гібридних загроз також може бути катастрофічним. Блокування доступу до міжнародних ринків, маніпуляції енергетичними ресурсами чи навмисне створення фінансових криз стають ефективними інструментами для послаблення економічної стабільності держави. Як видається, держави, які не мають стійкої економічної системи, є найбільш вразливими до таких загроз [10, с. 1–8].

2.3. Особливості гібридних загроз у контексті України. Національний досвід України є унікальним у контексті протидії гібридним загрозам. Від початку агресії з боку російської федерації держава стикається з багатовекторними викликами, які включають військові дії, кібератаки, економічний тиск і дезінформаційні кампанії. Дослідження, проведене А. Шишацьким та ін. [1, с. 26–29], вказує на важливість інтеграції сучасних технологій у систему національної безпеки як ефективного механізму протидії.

На наше переконання, особливу увагу слід приділяти розвитку співпраці з міжнародними партнерами, такими як НАТО та ЄС, які мають значний досвід у боротьбі з гібридними загрозами. Як зазначає С. Джунг [16, с. 1–22], регіональні ініціативи можуть стати дієвим інструментом для створення колективної безпеки, що є особливо актуальним для країн, які перебувають у зоні високого ризику.

З урахуванням викладеного вище, гібридні загрози становлять одну з найсерйозніших небезпек для національної безпеки, впливаючи на всі ключові сфери суспільного життя. Гадаємо, що їхнє усвідомлення та врахування у стратегіях безпеки є необхідним кроком для забезпечення стабільності та стійкості держави в умовах сучасних глобальних викликів. Тож узагальнимо результати осмислення й систематизації таких загроз в наступній таблиці.

Таблиця 1

Гібридні загрози: форми, ключові характеристики та можливі заходи протидії й відвернення

Форма гібридної загрози	**Ключові характеристики**	**Можливі заходи протидії й відвернення**
Військові загрози	Використання регулярних і нерегулярних військових формувань, територіальна анексія.	Підвищення обороноздатності, міжнародне співробітництво (НАТО), розвідка та моніторинг.
Інформаційні загрози	Дезінформація, маніпуляція громадською думкою, поширення фейкових новин.	Створення центрів протидії дезінформації, підвищення медіаграмотності, моніторинг ЗМІ.
Економічні загрози	Санкції, енергетична залежність, маніпуляції ринками, економічний шантаж.	Диверсифікація економіки, забезпечення енергетичної незалежності, розвиток локальних ринків.
Кіберзагрози	Кібератаки, зломи систем, втручання у критичну інфраструктуру.	Впровадження національних платформ кіберзахисту, міжнародні тренінги, посилення ІТ-інфраструктури.
Соціальні загрози	Провокація соціальної напруги, розпалювання етнічних і релігійних конфліктів.	Соціальні програми, інтеграція різних спільнот.

3. Стратегії протидії гібридним загрозам: міжнародний та національний виміри. У сучасному глобалізованому світі ефективна протидія гібридним загрозам потребує багаторівневих і скоординованих підходів, які поєднують зусилля держави, міжнародних організацій, приватного сектору та громадянського суспільства. На наше переконання, стратегія протидії повинна враховувати як унікальні національні особливості, так і міжнародний досвід, зокрема адаптацію найкращих практик, розроблених у рамках співпраці ЄС і НАТО [10, с. 1–8; 14, с. 209–226].

3.1. Міжнародні практики протидії гібридним загрозам. Європейський Союз та НАТО є провідними акторами у розробці механізмів протидії гібридним загрозам. У 2016 році ЄС ухвалив «Європейську рамкову стратегію протидії гібридним загрозам», яка передбачає інтеграцію інформаційних, кібернетичних та військових засобів у єдину систему безпеки. Як зазначає С. Санз-Кабальєро [10, с. 1–8], особлива увага приділяється посиленню співпраці між державами-членами та обміну інформацією для раннього виявлення загроз. На наше міркування, важливим уроком для інших держав є необхідність формування стійких комунікаційних каналів між різними рівнями управління.

НАТО, зі свого боку, акцентує на розвитку кібербезпеки як ключового елемента у боротьбі з гібридними загрозами. Як зазначає С. Джаспер [14, с. 209–226], використання сучасних технологій, таких як штучний інтелект і машинне навчання, дозволяє НАТО прогнозувати потенційні загрози та вживати заходів для їхньої нейтралізації. На наше переконання, адаптація цих технологій до національних контекстів є критично важливою для забезпечення ефективності стратегій безпеки.

Естонія є одним із прикладів успішної протидії гібридним загрозам завдяки створенню Центру передового досвіду НАТО з кібероборони у Таллінні. Як вказують Лушенко П. та ін. [12, с. 83–93], досвід Естонії демонструє, що ключовим фактором успіху є синергія між урядом, бізнесом і науковими колами. Цей підхід забезпечує постійне вдосконалення системи національної безпеки.

3.2. Національні стратегії України у протидії гібридним загрозам. Національна стратегія протидії гібридним загрозам в Україні формується на тлі багаторічної агресії з боку російської федерації, що включає як військові дії, так і масовані інформаційні атаки. Важливим елементом цієї стратегії є інтеграція міжнародного досвіду з урахуванням специфіки українського контексту. Як зазначають А. Шишацький та ін. [1, с. 26–29], ключовим напрямом є розробка ефективних механізмів раннього запобігання загрозам, що базуються на використанні великих даних і сучасних технологій.

В інформаційній сфері Україна активно впроваджує стратегії протидії дезінформації. Створення спеціалізованих державних органів, таких як Центр протидії дезінформації, є важливим кроком у цьому напрямі. На наше переконання, додаткову увагу слід приділити розробці освітніх програм для підвищення медіаграмотності населення, адже це дозволить зменшити вразливість суспільства до маніпуляцій [5, с. 57–78].

У сфері кібербезпеки Україна співпрацює з міжнародними партнерами, зокрема в рамках програми співпраці з НАТО. Як вказує С. Джунг [16, с. 1–22], розвиток спільних навчань і обмін досвідом з країнами-партнерами є ключовим фактором у формуванні ефективних механізмів кіберзахисту.

3.3. Інтеграція цифрових технологій у протидію гібридним загрозам. Цифрові технології відіграють вирішальну роль у сучасних стратегіях безпеки. Як зазначають Сидорчук О. та ін. [18, с. 747–759], інтеграція цифрових рішень у публічне управління дозволяє не лише підвищити ефективність реагування на загрози, але й мінімізувати наслідки

атак. Наприклад, розробка систем моніторингу інформаційного простору на основі штучного інтелекту дозволяє оперативно виявляти дезінформаційні кампанії.

На наше міркування, особливої уваги заслуговує питання створення національних платформ кіберзахисту, які могли б об'єднувати ресурси державного і приватного секторів. Як показує досвід країн ЄС, тісна співпраця між різними суб'єктами є ключовим фактором у протидії гібридним загрозам [10, с. 1–8].

Висновки. Дослідження феномена гібридних загроз у контексті національної безпеки дозволило зробити низку теоретичних і практичних висновків, які мають важливе значення для розробки ефективних стратегій протидії сучасним викликам. На наше переконання, багатовимірність цього явища зумовлює необхідність інтегрованого підходу, що враховує специфіку кожної частини – військової, інформаційної, економічної та кібербезпеки.

По-перше, гібридні загрози є унікальним типом сучасних викликів, які поєднують видимі й приховані методи впливу, спрямовані на підрив національної безпеки. Гадаємо, що їхня багатовекторність та адаптивність ставлять під сумнів ефективність традиційних підходів до забезпечення безпеки, зокрема у сфері інформаційної та кібербезпеки.

По-друге, аналіз міжнародного досвіду протидії гібридним загрозам (зокрема, практик ЄС, НАТО та окремих країн, таких як Естонія) свідчить про важливість колективних зусиль у боротьбі з цим явищем. На наше переконання, співпраця між державами, а також міждержавними та недержавними акторами є ключовим елементом у формуванні стійких систем захисту.

По-третє, український контекст боротьби з гібридними загрозами демонструє, що ефективна протидія потребує не лише адаптації міжнародного досвіду, але й розробки унікальних підходів, що враховують специфіку внутрішніх і зовнішніх факторів. Зокрема, створення національних інституцій для протидії дезінформації, активна співпраця з міжнародними організаціями у сфері кібербезпеки та впровадження цифрових технологій є важливими етапами на цьому шляху.

По-четверте, інтеграція цифрових технологій у стратегії протидії гібридним загрозам є критично важливою. На наше міркування, використання штучного інтелекту, машинного навчання та великих даних дозволяє створити ефективні механізми моніторингу й раннього запобігання загрозам, що значно підвищує рівень національної стійкості.

Таким чином, комплексний підхід, що поєднує міжнародні практики, міждисциплінарні методи та врахування національних особливостей, є основою для ефективної протидії гібридним загрозам. Гадаємо, що розвиток таких стратегій є необхідним для забезпечення стабільності та безпеки у сучасному світі, що стикається зі зростанням транснаціональних викликів. З урахуванням викладеного вище, подальші дослідження у цій сфері повинні зосереджуватися на пошуку інноваційних рішень, здатних адаптуватися до швидкозмінного характеру гібридних конфліктів.

Список використаної літератури

1. Shyshatskyi A., Hurskyi T., Vdovytskyi Y., Vozniak R., Nalapko O., Andriishena H., ... & Pyvovarchuk S. Development of method for the identification of hybrid challenges and threats in the national security management system. Technology audit and production reserves. 2023. Vol. 2(2/70). P. 26–29.
2. Mitrovic M. Hybrid Security Threats and Contemporary Approach to National Security. Thematic Conference Proceedings of International Significance, International Conference «Archibald Reiss Days», Academy of Criminal and Police Studies, Belgrade. 2017. Vol. 1. P. 337–345.

3. Bratko A., Zaharchuk D., & Zolka V. Hybrid warfare – a threat to the national security of the state. Revista de Estudios en Seguridad Internacional. 2021. Vol. 7(1). P. 147–160.
4. Cilluffo F. J., & Clark J. R. Thinking about strategic hybrid threats–in theory and in practice. Prism. 2012. Vol. 4(1). P. 46–63.
5. Tsaruk O., & Korniiets M. Hybrid nature of modern threats for cybersecurity and information security. Smart Cities and Regional Development (SCRD) Journal. 2020. Vol. 4(1). P. 57–78.
6. Taneski N., & Kirkova R. The concept of hybrid threats. Knowledge-International Journal, Scientific Papers. 2018. Vol. 28. P. 1795–1800.
7. Bielai S., Emanov V., Trobiuk V., Sporyshev K., & Petik A. Improvement of public management mechanisms in the direction of countering hybrid threats to national security. Edelweiss Applied Science and Technology. 2024. Vol. 8(6). P. 1312–1321.
8. Kovalchuk T. I., Korystin O. Ye., Sviridyuk N. P. Hybrid threats in the civil security sector in Ukraine. Проблеми законності. 2019. Вип. 147. С. 163–175.
9. Cullen P. Identifying hybrid threats from a national security perspective: The case of Chinese hybrid threats in Australia. Preparing for Hybrid Threats to Security. Routledge. 2024. P. 52–66.
10. Sanz-Caballero S. The concepts and laws applicable to hybrid threats, with a special focus on Europe. Humanities and Social Sciences Communications. 2023. Vol. 10(1). P. 1–8.
11. Balcaen P., Du Bois C., & Buts C. Sharing the burden of hybrid threats: Lessons from the economics of alliances. Defence and Peace Economics. 2023. Vol. 34(2). P. 142–159.
12. Lushenko P., Bose S., & Romaniuk S. N. Blending Counterinsurgency to Defeat Hybrid Threats. Handbook of Terrorist and Insurgent Groups. CRC Press. 2024. P. 83–93.
13. Razali N. A. M., Malizan N. A., Hasbullah N. A., Wook M., Zainuddin N. M., Ishak K. K., ... & Sukardi S. Political security threat prediction framework using hybrid lexicon-based approach and machine learning technique. IEEE Access. 2023. Vol. 11. P. 17151–17164.
14. Jasper S. Resilience against hybrid threats: Empowered by emerging technologies: A study based on Russian invasion of Ukraine. Handbook for Management of Threats: Security and Defense, Resilience and Optimal Strategies. Cham: Springer International Publishing. 2023. P. 209–226.
15. Harris K. A hybrid threat: The Night Wolves motorcycle club. Studies in Conflict & Terrorism. 2023. Vol. 46(9). P. 1784–1816.
16. Jung S. C., & Tan E. W. Middle powers and minilateralism against hybrid threats in the Indo-Pacific: South Korea, Singapore, and Taiwan. Australian Journal of International Affairs. 2024. P. 1–22.
17. Schmid J. Political Islamism–A Vital Hybrid Threat/Challenge. Handbook of Political Islam in Europe: Activities, Means, and Strategies from Salafists to the Muslim Brotherhood and Beyond. Cham: Springer International Publishing. 2024. P. 59–79.
18. Sydorchuk O., Bashtannyk V., Terkhanov F., Kravtsov O., Akimova L., & Akimov O. Integrating digitization into public administration: Impact on national security and the economy through spatial planning. Edelweiss Applied Science and Technology. 2024. Vol. 8(5). P. 747–759.

HYBRID THREATS AS A NEW CHALLENGE TO NATIONAL SECURITY IN THE ERA OF INFORMATION WARS

Andriy Krap
Interregional Academy of Personnel Management,
Department of Social and Humanitarian and Fundamental Disciplines
Frometovskaya str., 2, 03039, Kyiv, Ukraine

The article explores the phenomenon of hybrid threats as a complex challenge to national security in the context of the modern era of information wars. The study aims to conceptualize hybrid threats, determine their nature, identify key forms of manifestation and consequences, and propose effective counter-strategies. Special attention is given to the impact of hybrid threats on state institutions, economic stability, and the information sphere.

The study employs an interdisciplinary approach, integrating methods of systems analysis, historical-genetic methodology, comparative analysis, and critical evaluation of legal frameworks. This comprehensive approach has allowed for the development of a holistic understanding of the multidimensional nature of hybrid threats and the delineation of methods for their neutralization.

The main results of the article include: characterization of the multidimensional nature of hybrid threats; analysis of key forms of manifestation (military, informational, economic, and cyber components); identification of the consequences of hybrid threats for national security; review of international counteraction practices (e.g., the EU, NATO, and Estonia) and their adaptation to the Ukrainian context; proposals for integrating digital technologies into national security strategies.

The scientific novelty of the article lies in the formation of a comprehensive approach to studying hybrid threats and developing recommendations for their effective neutralization. The theoretical significance of the study is reflected in the generalization and systematization of contemporary concepts of hybrid threats, contributing to further research in this field. The practical value lies in the formulation of recommendations to improve state policy in the area of national security.

Key words: hybrid threats, national security, information war, cybersecurity, disinformation, international cooperation, digital technologies.